IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX INC.	§	
	§	**CASE NO. 607CV80 (LED)**
PLAINTIFF,	§	**PATENT CASE**
	§	
AND	§	
	§	**JURY TRIAL DEMANDED**
SCIENCE APPLICATIONS	§	
INTERNATIONAL CORPORATION	§	
	§	
INVOLUNTARY	§	
PLAINTIFF,	§	
	§	
V.	§	
MICROSOFT CORPORATION	§	
	§	
DEFENDANT.		

PLAINTIFF VIRNETX INC.'S OPENING BRIEF IN SUPPORT OF ITS CONSTRUCTION OF CLAIMS PURSUANT TO P.R. 4-5

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

LIST OF EXHIBITS TO VIRNETX'S OPENING CLAIM CONSTRUCTION BRIEF

1. '135 patent
2. '759 patent
3. '180 patent
4. Jones declaration
5. Williamson deposition
6. FreeS/WAN glossary
7. Risley '158 patent
8. Office Action (Paper No. 8) dated March 13, 2002
9. Amendment and Response (Paper No. 11) dated June 13, 2002
10. WO 99/48303
11. B. Gleeson et al., Request for Comments (RFC) 2764
12. Douglas E. Comer, Computer Networks and Internets (2d ed. 1999)
13. Microsoft Internet & Networking Dictionary (2003)
14. Microsoft document (VNET 000008935)
15. RFC 1034
16. RFC 1035
17. McGraw-Hill Dictionary of Electrical & Computer Engineering (2003)
18. Andrew S. Tanenbaum, Computer Networks (3d ed. 1996)
19. Notice of Allowability (Paper No. 13)
20. U.S. Patent No. 6,119,171
21. U.S. Patent No. 6,286,047
22. J. Gilmore, "Swan: Securing the Internet against Wiretapping", printed from http://liberty.freeswan.org/freeswan_trees/freesswan-1.3/doc/rationale. html on Feb. 21, 2002, 4 pages

23. Second Preliminary Amendment (Paper No. 9) dated February 22, 2002

24. Notice of Allowability dated August 9, 2004

25. Merriam Webster's Collegiate Dictionary (10th ed. 1996)

26. Amendment dated August 17, 2006

27. Notice of Allowability dated November 13, 2006

28. Dr. D. Johnson deposition rough transcript

29. RFC 2637

30. RFC Index

I. INTRODUCTION

A consistent theme emerges from examination of the parties' competing constructions. VirnetX's proposed constructions give full scope to the claim language, as firmly supported by the intrinsic evidence. Microsoft's proposed constructions, however, seek to limit the claims to certain preferred embodiments (while excluding others), to extrinsic industry standards, or to extrinsic dictionary definitions that conflict with the context of the patented inventions. The canons of claim construction favor VirnetX's proposed constructions and compel rejection of Microsoft's.

II. APPLICABLE CLAIM CONSTRUCTION STANDARDS

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*) (internal citation omitted). The specification "'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* at 1315 (internal citation omitted). The prosecution history also supplies intrinsic evidence if it is in evidence. *Id. at* 1317. "Differences among the claim terms can also assist in understanding a term's meaning … For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation." *Alcatel United States Res., Inc. v. Microsoft Corp.*, 2008 U.S. Dist. LEXIS 49615, at *5 (E.D. Tex. Jun. 27, 2008). "Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent." *Id.* at *7. Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

III. BACKGROUND OF THE TECHNOLOGY

The field of the three VirnetX patents in suit is secure computer network communications, more specifically, communications in a virtual private network (VPN). As will be seen, the three VirnetX patents are directed to aspects of using a domain name service (DNS) or secure domain name service (SDNS) to set up and use VPNs.

A. VirnetX's U.S. Patent No. 6,502,135 (the "'135 Patent")

The '135 patent improves security in computer networks through a novel method and system of creating VPNs. Networks, such as VPNs, can carry all kinds of traffic between computers using various applications and protocols. A VPN, in particular, allows computers in a network to communicate privately by encrypting their communications on paths between them that may be insecure, *e.g.*, over underlying public networks, such as the Internet, that may be subject to nefarious listeners. *See '135 patent* (Exhibit 1 hereto) at 1:16-45; 37:40-49.

There were several problems with the prior art. One category of prior art required a user to manually set up the VPN, such as by providing encryption information, *e.g.*, keys required to encrypt and decrypt the messages. *Ex.* 4 (Jones Decl.) ¶22; *Ex. 5* (Williamson rough Depo. Tr.) at 46-47. However, manually created VPNs were neither flexible nor easy to use. For example, business travelers trying to remotely connect to their corporate networks through VPNs had difficulty setting up and using VPNs. *See '135 patent* at 2:52-63.

The '135 patent improves security by making it easier for users to use VPNs without the user having to manually create the VPN, and ensuring VPNs are created when they are needed, without compromising security, *e.g.*, for business travelers who need to establish VPNs with their corporate networks over the Internet. *See id.* at 5:8-12; 11:39-43. The '135 patent claims a method and system of "transparently creating a virtual private network (VPN)." *See '135 patent* claims 1 and 10. In other words, a user need not be involved in creating the VPN. *See id.* at 39:22-29. The inventions transparently create the VPN by initiating or setting up the VPN in response to a DNS request. *Id.* at 6:1-3; 32:33-35; 37:17-21; 37:63-38:2. Put another way, a DNS request triggers a VPN. *Id.* A DNS request contains a domain name, one example of which is "Yahoo.com." *Id.* at 37:22-29; 37:45. A DNS request is to be sent to a DNS, which is a service that receives requests for computer network addresses (machine-understandable numerical addresses) corresponding to domain names, and which provides responses. *See '135 patent* at 37:22-29; 37:45; 38:23-42. As claimed in claims 1 and 10, the invention can examine the DNS request and determine whether to create the VPN for the user based on the DNS request. In system claim 10, in response to the DNS request, a DNS proxy server requests a VPN for the user and a gatekeeper computer allocates the resources for the VPN.

B. VirnetX's U.S. Patent No. 6,839,759 (the "'759 Patent")

The '759 patent stems from a continuation-in-part of the '135 patent and provides further improvements in security in computer networks through another novel method and apparatus of controlling who can establish VPN links using DNS without a user entering cryptographic information, such as encryption keys. *See '759 patent* (Exhibit 2 hereto) Title; claims 1 and 16; 6:37-51; *see also id.* 6:21-36. The prior art failed to differentiate between requestors in deciding whether to set up a VPN. *Id.* at 40:24-37. This was a significant drawback in the prior art. *Id.* The invention overcomes the problems of the prior art. The invention provides a DNS that provides VPN resources based on the requestor's (or user's) identity. *Id.* at 40:37-44. If the requestor does not have sufficient security privileges to communicate in a VPN, the VPN will not be enabled. *Id.* at 40:48-55; 41:23-28; 41:51-64; 41:65-42:2; 42:19-38; Fig. 27.

C. VirnetX's U.S. Patent No. 7,188,180 (the "'180 Patent")

The '180 patent (which shares the same specification as the '759 patent) provides further improvements in security in computer networks through another novel method and apparatus of using a secure domain name service (SDNS) to provide secure computer network addresses corresponding to secure domain names and enable a VPN communication. *See '180 patent* (Exhibit 3 hereto) Title; claims 1, 17 and 33; 6:22-37; 7:19-42. The prior art did not provide for such a SDNS. *Id.* at 6:22-36. In an embodiment of the invention, secure domain name requests (for secure computer network addresses) are handled by a SDNS. *Id.* at 51:28-45; 53:26-40. The SDNS has a registry of secure domain names. Figure 35 shows an embodiment of registering a secure domain name with a SDNS. *Id.* at 53:26-54:6. *Id.* at 52:22-26; 52:41-46. The SDNS provides additional security. It is capable of providing trustworthy responses, *e.g.*, by replying to the secure domain name request with the secure computer network address using a VPN link. *Id.* at *Id.* at 52:4-22; 52:37-40; 52:51-54; Fig. 34.

IV. VIRNETX'S PROPOSED CONSTRUCTIONS FOR THE '135 PATENT CLAIM TERMS AND PHRASES SHOULD BE ADOPTED.

Method claim 1 contains seven of the eight disputed claim terms and phrases in the '135 patent, in bold and underlining below:[1]

> 1. A method of **transparently creating a <u>virtual private network (VPN)</u>** between a client computer and a target computer, comprising the steps of:
>
> (1) generating from the client computer a **Domain Name Service (DNS)** request that requests an IP address corresponding to a **domain name** associated with the target computer;
>
> (2) **determining whether the <u>DNS</u> request transmitted in step (1) is requesting access to a <u>secure web site</u>**; and
>
> (3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, **automatically initiating the <u>VPN</u>** between the client computer and the target computer.

System claim 10, the other independent claim in the patent, contains six of the eight disputed claim terms and phrases (including the additional term "DNS proxy server"), in bold and underlining below:

> 10. A system that **transparently creates a <u>virtual private network (VPN)</u>** between a client computer and a secure target computer, comprising:
>
> a **<u>DNS</u> proxy server** that receives a request from the client computer to look up an IP address for a **domain name**, wherein the DNS proxy server returns the IP address for the requested domain name if it is determined that access to a non-secure web site has been requested, and wherein the DNS proxy server generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a **secure web site** has been requested; and
>
> a gatekeeper computer that allocates resources for the **VPN** between the client computer and the secure web computer in response to the request by the DNS proxy server.

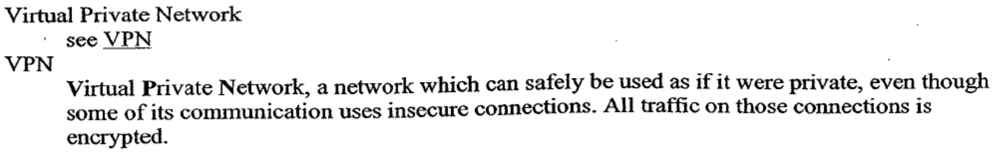
A. virtual private network (VPN)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a network of computers capable of privately communicating with each other by encrypting traffic on insecure communication paths between the computers, and which is capable of expanding to include additional computers and communication paths	a network implemented by encapsulating an encrypted IP packet within another IP packet (that is, tunneling) over a shared networking infrastructure

[1] Disputed terms and phrases are only highlighted once in the claims herein.

The dispute about the construction of the claim term "virtual private network (VPN)" is whether the intrinsic evidence explicitly defining the term should control the construction, as proposed by VirnetX, or whether Microsoft's restrictive construction, limiting VPNs to a particular protocol and specific packet format (encapsulation of one IP packet within another) trumps the explicit (and industry-accepted) definition provided in the intrinsic evidence. VirnetX's intrinsic evidence definition should be adopted.

VirnetX's Proposed Construction. The claim language itself is of limited assistance in defining the term VPN since the claim language does not tell us what a VPN is. The first part of VirnetX's proposed construction is "a network of computers capable of privately communicating with each other by encrypting traffic on insecure paths between the computers." The intrinsic evidence contains an explicit definition of a VPN that supports VirnetX's construction. The specification refers to the "FreeS/WAN" project as the conventional scheme of creating a "VPN." *'135 patent* at 37:50-62. The prosecution history file prominently includes a FreeS/WAN glossary of terms defining a VPN. *See Acumed LLC v. Stryker Corp.*, 483 F.3d 800, 815 (Fed. Cir. 2007) (intrinsic evidence includes references cited during prosecution). The FreeS/WAN glossary defines a VPN as follows:



Virtual Private Network
see VPN
VPN
Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.

Ex. 6 at 24. As can be seen, the definition of a VPN includes encrypting traffic on insecure paths (or connections) between computers in the network, allowing the computers to privately communicate with each other. The VPN provides security by encrypting traffic communicated between computers in the VPN, and "[m]any encryption methods are known and usable in this context." *'135 patent* at 1:38-45; 37:63-38:2; *see also id.* at 38:13-22; 38:43-52; 39:7-20; 39:21-25; 39:42-60. Moreover, consistent with the FreeS/WAN glossary definition of a VPN, Figure 24 in the specification shows that there can be multiple paths in the VPN (rather than just one path).

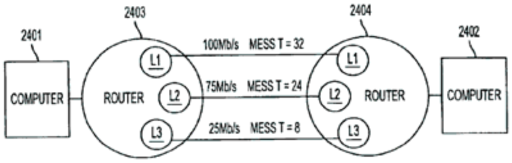


FIG. 24

Id. at 36:25-32 (links L1, L2 and L3 may be VPN links); Fig. 24. This intrinsic evidence supports this part of VirnetX's construction that a VPN is "a network of computers capable of privately communicating with each other by encrypting traffic on insecure paths between the computers."

The intrinsic evidence also supports the second part of VirnetX's proposed construction of a VPN as "capable of expanding to include additional computers and communication paths." The intrinsic evidence establishes that a VPN, as a network, must include the capability of expansion, also known as scalability. The specification describes an embodiment of a VPN as including more than two computers or nodes. *'135 patent* at 23:11-20; 29:30-64. In addition, the cited art (the Risley '158 patent) describes and depicts a "typical network" as including more than two computers. *Ex.* 7 at 5:62; Fig. 2C. The Risley '158 patent was relied upon by the Examiner in support of a rejection, which was overcome based on the '135 patented invention's use of a DNS request to trigger a VPN. *Ex.* 8; *Ex.* 9 at 6 ("Neither Risley nor Boden teach or suggest triggering the creation of a VPN in response to a DNS request."). Another cited reference describes a VPN as expandable, noting that "new locations" can be "easily added to the network." *Ex.* 10 at VNET 00221857. Thus, while the patent describes VPNs between a client and target computer, this connection must be scalable to add additional computers (nodes).

The extrinsic evidence is consistent. A VPN emulates the scalability of a WAN. *See Ex.* 11 at 4 ("[A] ***VPN*** is simply defined as ***the*** '***emulation of a Wide Area Network (WAN) facility*** using IP facilities' (including the public Internet, or private IP backbones).") (emphasis added); *Ex.* 12 at 168 ("***The key issue*** that separates ***WAN technologies*** from LAN technologies is ***scalability*** – a WAN must be able to grow as needed to connect many sites spread across large geographic distances, with many computers at each site.").

Microsoft's Proposed Construction. Microsoft's construction is unnecessarily narrow and conflicts with the intrinsic evidence definition as well as examples in the specification. It requires encapsulation of an IP packet within another IP packet, and thus excludes networks other than over the Internet, and other packets. The specification, however, describes VPNs which are implemented without such encapsulation, and in networks other than the Internet, such as Ethernet. *'135 patent* at 23:11-36. As the other intrinsic evidence indicates, encapsulation of a packet within another IP packet is possible, but not required. *Ex.* 7 at 7:44-49 ("Encryption and decryption may also automatically be executed on certain data packets, with the criteria defined by the system administrator. Along with this ***it may be desirable*** to encapsulate a packet and give it a new header with a new IP address …") (emphasis added). Consistent with the intrinsic evidence, Microsoft's dictionary definition of a VPN does not include any of the encapsulating or tunneling limitations it seeks to impose on VirnetX. *Ex.* 13 at 278 ("Nodes on a public network such as that Internet that communicate among themselves using encryption technology so that their messages as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines").

Microsoft makes a convoluted argument that the VPN must be based in the IP layer.[2] *Joint Claim Construction Statement* ("JCC") *Exh. E* ¶¶31-34. The purported basis for this argument is that "[t]he patents-in-suit distinguish between VPNs [allegedly at the networking layer] and so-called 'virtual private connections' [allegedly at the application layer]." *Id.* ¶ 31. The described virtual private connection, upon which Microsoft's argument hinges, does not even use encryption. *'180 patent* at 54:24-29; 55:2-14; 55:37-46; Fig. 37. Even Microsoft agrees that a VPN must employ some type of encryption, so the layer at which an unencrypted virtual private connection is implemented is irrelevant to the definition of a VPN. Moreover, it is notable that the citations on which Microsoft relies for this alleged distinction are only in the '759 and '180 patents, and not the earlier-filed '135 patent. The term "virtual private network" or "VPN" is found first and foremost in the '135 patent.

[2] Microsoft's motivation for seeking to unduly limit the virtual private network (VPN) in the claims to "encapsulating," "tunneling" and encrypting at the IP networking layer is to try to exclude VPNs using technologies like Secure Socket Layer (SSL) or Transport Layer Security (TLS), used by Microsoft's accused products. *JCC Exh. E* ¶31.

The common denominator of the patents in suit is the FreeS/WAN glossary definition of a VPN on which VirnetX relies, which has none of Microsoft's encapsulating or tunneling limitations.

Additionally, Microsoft's reliance on the '135 patent's description of IPSEC, as well as address hopping, is misplaced. In fact, the specification distinguishes the only implementation of IPSEC described, the conventional prior art FreeS/WAN scheme of creating a VPN. *'135 patent* at 37:22-62. In any event, the FreeS/WAN glossary defines a "VPN" as proposed by VirnetX. Moreover, the specification describes "address hopping," the preferred embodiment (*id.* at 38:1-6), as implemented in networks not limited to the Internet, such as Ethernet networks, so encapsulation of an IP packet within another IP packet at the Internet network layer is not the only kind of VPNs described by the specification. *Id.* at 19:25-36; 19:37-47; 20:62-66; 21:41-49; 29:30-64; 38:2-6; 38:33-35. The VPN packets in the preferred embodiment are not limited to IP packets with IP headers, and other packets and headers can be used to implement the VPN, such as MAC addresses. *Id.* at 9:43-49; 10:59-62; 18:31-37; 18:42-44; 19:47-20:3; 20:32-66; 21:3-29; 22:40-44; 23:11-20; 23:45-59; 29:30-64; 43:29-39. The preferred embodiment VPNs can thus be implemented in layers other than the IP network layer. *Id.* at 10:63-66; 19:37-47; Fig. 12A. A construction like Microsoft's that excludes an embodiment, without any kind of lexicography, disclaimer or disavowal, is not correct. *See Verizon Servs. Corp.. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1305 (Fed. Cir. 2007) ("We normally do not interpret claim terms in a way that excludes disclosed examples in the specification."); *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008) (same).

In addition, to the extent extrinsic sources are considered, it should be noted that Microsoft co-authored a standard on VPNs (known as PPTP) which were not limited to tunneling by encapsulating an IP packet within another IP packet. *Ex.* 29 at 4 (describing IPX and Appletalk). Indeed, the word "tunneling" in the art is more general and is used to describe other kinds of packets encapsulated in other packets; *i.e.*, not all VPNs are IP based. *Ex.* 4 (*Jones Dec.*) ¶21. *See also Ex.* 11 ("A Framework for ***IP Based*** Virtual Private Networks") (emphasis added).

In any event, the word "tunneling" in Microsoft's construction is not instructive and could be confusing for the jury.

VirnetX's proposed construction includes every aspect of what it means to have a VPN, as defined in the intrinsic evidence. Microsoft's definition, however, includes unwarranted limitations. VirnetX's proposed construction is the correct construction.

B. transparently creating [creates] a virtual private network (VPN)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a user need not be involved in creating a virtual private network (VPN)	no construction necessary because the preamble is not a limitation. In the alternative, to the extent the court determines a construction is necessary, it is "creating a virtual private network (VPN) without the client or target computer involved in requesting such creation"

The dispute about the construction of the claim phrase is whether the "transparently …" phrase is a limitation of the claim and whether the intrinsic evidence defines the word "transparently" as not requiring user involvement as proposed by VirnetX, or whether the word "transparently" requires no construction, as proposed by Microsoft. The '135 patent defines the word "transparently" as VirnetX proposes, and this meaning is a critical aspect that gives life and meaning to the claimed invention. But, even if the "transparently …" phrase is not a limitation, it should be construed as VirnetX proposes to help the jury and avoid any confusion.

VirnetX's Proposed Construction. The claim language itself makes it clear that the "transparently …" phrase is part of the invention. Claims 1 and 10 are directed to creating a VPN between a client computer and target computer, as seen in both the preamble and body of the claims. Antecedent basis for the terms VPN, client computer and target computer are found in the preamble. *See Electro Sci. Indus. v. Dynamic Details, Inc.*, 307 F.3d 1343, 1348 (Fed. Cir. 2002); *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305-06 (Fed. Cir. 1999) (preamble limiting because it is "intimately meshed with the ensuing language in the claim" even though not all preamble terms are recited in the body of the claim) (internal citations omitted). Further, the claim language shows that a user need not be involved in creating the VPN. In claim 1, the VPN is created in response to a DNS request. In claim 10, a DNS proxy server requests creation of the VPN, and a gatekeeper computer allocates resources for the VPN.

The Abstract, the Summary of the Invention and the Detailed Description describe the invention in terms of transparently creating a VPN in response to a domain name inquiry (or query), a DNS request. *'135 patent* at Abstract; 6:1-3; 7:18-23; 32:33-35; 37:17-21; Figs. 26, 27. In an act of lexicography, the specification then specifically defines the word "transparently" to the user as "the user need not be involved in creating the secure link." *Id.* at 39:21-29. Instead of a user being involved in created a secure link in a VPN, "transparent VPN creation" is "based on a DNS look-up function." *Id.* at 7:22-23. The prosecution history then consistently distinguishes the prior art as <u>not</u> creating a VPN in response to a DNS request. *Ex.* 9 at 3-6.

Microsoft's Proposed Construction. Microsoft's argument that the phrase "transparently …" is not a part of the invention ignores all of the intrinsic evidence above. But, even if the Court agrees that the phrase is not a limitation of the claim, the Court should construe the phrase to help the jury. Without construction by the Court, the jury could be confused and think that the word "transparently" means that something can be "seen through," such as a window.

Microsoft proposes the following alternative definition: "creating a virtual private network (VPN) without the client or target computer involved in requesting such creation." This limitation has no support in the intrinsic or extrinsic evidence and is wrong for at least two reasons. First, Microsoft's proposed limitation does not relate to the user, contrary to the specification's description that the word "transparently" means the user need not be involved in creating the VPN. *'135 patent* at 39:21-29. Second, there is nothing in the claim language that says the client or target computer cannot be involved in creating the VPN. On the contrary, the client computer can be involved by issuing the DNS request. Moreover, dependent claims indicate that the client computer may be involved in creating the VPN. Claim 12 (which depends on claim 10) recites "[t]he system of claim 10, wherein the gatekeeper computer determines whether the ***client computer has sufficient security privileges to create the VPN*** and, if the client computer lacks sufficient security privileges, rejecting ***the request to create the VPN***." *Id.* at 48:25-29 (emphasis added). Similarly, claim 2 (which depends on claim 1) recites "[t]he method of claim 1, wherein steps (2) and (3) are performed at a DNS server separate from the client computer." *Id.* at 47:33-35. Step (3) of claim 1 includes "automatically initiating the VPN between the client computer and the target computer." Claim 2 thus indicates that the functionality in claim 1, which includes initiating the VPN, can be on the client computer. *Id.* at 47:29-33.

VirnetX's proposed construction of the "transparently" phrase is firmly supported by the intrinsic evidence, particularly the inventors' own lexicography in the specification itself, which must control over Microsoft's unwarranted limitations.

C. Domain Name Service (DNS)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a service that receives requests for computer network addresses corresponding to domain names, and which provides responses	the conventional lookup service defined by the Internet Engineering Task Force that returns the IP address of a requested computer or host

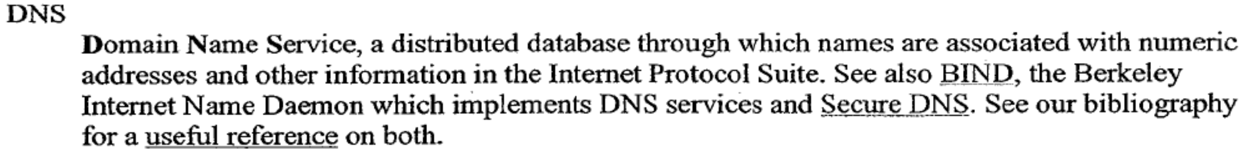
The dispute about the construction of the claim term "Domain Name Service (DNS)" is whether a DNS includes characteristics of both the conventional DNS and modified DNS described in the specification, as proposed by VirnetX, or whether it is limited to the Internet Engineering Task Force (IETF) implementation extrinsic to the patent, as proposed by Microsoft. VirnetX's construction is proper because the specification describes multiple forms of DNS, and there is no reason to limit the scope of the term to any particular implementation extrinsic to the patent.

VirnetX's Proposed Construction. The claim language in both claims 1 and 10 indicates that the DNS is "a service that receives requests for computer network addresses corresponding to domain names, and which provides responses," as proposed by VirnetX. Claim 1 says "generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer." Claim 10 says "a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name …"

The specification describes both a conventional DNS and another form of DNS, a modified form of DNS "[a]ccording to one embodiment." *'135 patent* at 38:23-33. The conventional DNS is described as providing a "look-up function that returns the IP address of a requested computer or host." *Id.* at 37:22-24. In a preferred embodiment, the specification then goes on to describe a "modified

DNS server" which includes both a "conventional DNS server function" and other DNS server functionality. *Id.* at 38:17-19. "According to one embodiment," the modified DNS server (or DNS proxy) can handle either conventional DNS requests or modified domain names (*e.g.*, domain name extensions) to set up a VPN. *Id.* at 38:23-33. Moreover, the DNS may not return the IP address of the destination computer, but may return the message "host unknown" instead if the user is not authorized to connect to a secure site. *Id.* at 38:43-52; 39:21-25; 39:53-60. Thus, VirnetX's proposed construction that the DNS "provides responses" is appropriate.

The prosecution history includes the FreeS/WAN glossary, which defines DNS as follows:



DNS

Domain Name Service, a distributed database through which names are associated with numeric addresses and other information in the Internet Protocol Suite. See also BIND, the Berkeley Internet Name Daemon which implements DNS services and Secure DNS. See our bibliography for a useful reference on both.

Ex. 6 at 9. This is consistent with VirnetX's proposal. Notably, the FreeS/WAN glossary's definition of "DNS" does not include any citation to Requests for Comments (RFCs) by the IETF, contrary to Microsoft's proposal. Further, the glossary's use of "See also" in referencing the "BIND" implementation of DNS indicates that there are many implementations of DNS, and that the term DNS itself is not limited to any particular implementation.

Microsoft's Proposed Construction. Microsoft's proposed construction limiting the term to the DNS defined by the IETF RFCs is contrary to the specification and therefore improper. As an initial matter, Microsoft admits that the use of the capital letters in "DNS" is insignificant in defining the term. *JCC Exh. E*, ¶8. Microsoft limits the term to the DNS as defined by the IETF, excluding the specification's description of a modified form of DNS handling domain name requests in the form of domain name extensions, "[a]ccording to one embodiment." *See '135 patent* at 38:23-33.

Microsoft argues that the invention requires "the standard DNS protocols defined in the IETF RFCs in order to work." *JCC Exh. E*, ¶12. But there is no basis in the patents for this. There is no reason why domain name service protocols other than those defined in the IETF RFCs cannot work. *Ex.* 4 (*Jones Decl.*) ¶32. Microsoft admits that there are other forms of DNS. *JCC Exh. E* ¶9. Microsoft further admits that a DNS converts computer names into computer addresses. *Id.* There is no basis to limit the DNS in the claims to one particular implementation extrinsic to the patents, the IETF RFCs.[3]

In addition, Microsoft's construction is so complicated that it would not be helpful to the jury and indeed would need a construction of a construction. Microsoft cannot expect the jury to look at what is "defined by the Internet Engineering Task Force," and then apply that to the accused instrumentalities. Microsoft points to RFCs 1034 and 1035, but there are many related standards defined by the IETF in the form of RFCs. *Ex.* 4 (*Jones Decl.*) ¶24; *Ex.* 30 at 3. Even if the jury was expected to look at IETF RFCs 1034 and 1035 cited by Microsoft, what are they supposed to consider within Microsoft's definition among the ***more than 100 pages*** in those RFCs? *Ex.* 15; *Ex.* 16. What among these are required under Microsoft's construction? Microsoft's argument appears to assume this Court will hand over its power to construe the claim limitation to the experts in this case – with Microsoft's expert construing the IETF standard, and telling the jury if the standard is met by the accused products. *See Ex.* 28 (Johnson Depo.) at 142-147.[4] It is the Court's role to construe the claims. Adopting Microsoft's construction hands over that responsibility to the experts. Microsoft's construction also ignores the fact that the IETF can change its definition of "DNS". There is no basis in the intrinsic evidence for Microsoft's IETF limitation, and this is not helpful to the jury, the Court, or the parties. It would be error to construe the term, as Microsoft does, in a way that invites further disputes between the parties about the meaning of the term in front of the jury, or a definition that changes according to the IETF. *See O2 Micro Inter. Ltd. v. Beyond Innovation Tech. Ltd.*, 521 F.3d 1351, 1360 (Fed. Cir. 2008).

Finally, Microsoft's proposal that the DNS "returns the IP address of a requested computer or host" is directly contradicted by the specification. In some cases, the DNS may return the IP address of

[3] Microsoft's motivation for seeking to unduly limit the domain name service (DNS) in the claims to the IETF RFCs is to try to exclude other domain name resolution protocols that allegedly do not correspond to the specific RFCs identified by Microsoft, including Microsoft's Peer Name Resolution Protocol (PNRP). *JCC Exh. E* ¶12. This is ironic given that Microsoft itself has admitted that its PNRP is a DNS before this case. *Ex.* 14 (VNET 000008935).

[4] Citations to the Johnson deposition transcript are citations to the rough transcript as the parties await the final transcript.

the destination computer, but in others it may not; instead, it may return the message "host unknown." *'135 patent* at 38:43-52; 39:21-25; 39:53-60.

VirnetX's proposed construction should be adopted as supported by the intrinsic evidence of a DNS that encompasses both conventional and other forms of DNS, whereas Microsoft's should be rejected as unduly limiting the term to an extrinsic, undefined implementation by the IETF.

D. domain name

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a series of characters that corresponds to an address of a computer or group of computers that is to be sent to a domain name service (DNS)[5]	a hierarchical name for a computer (such as www.utexas.edu) that the Domain Name Service converts into an IP address

The dispute about the construction of the claim term "domain name" is whether the term includes a name corresponding to either a computer or group of computers, as proposed by VirnetX, or is limited to a specifically formatted name ("hierarchical") corresponding to a particular kind of computer, a computer providing web pages ("such as www.utexas.edu"), all on the World Wide Web, as proposed by Microsoft. The intrinsic evidence favors VirnetX's construction over Microsoft's unduly limited construction.

VirnetX's Proposed Construction. The claim language supports VirnetX's construction. The claims expressly indicate that a "domain name" is "to be sent to a domain name service (DNS)." Claim 1 recites "a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer." Similarly, claim 10 recites "a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name." Further, by reciting "an" IP address, rather than "the" IP address, the claim language indicates that there may be more than one IP address (and therefore more than one computer) corresponding to the domain name. *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1343 (Fed. Cir. 2008).

The specification describes a "domain name" as "to be sent to a domain name service (DNS)." *'135 patent* at 37:63-38:65. The specification also describes domain names as corresponding to "a

[5] To try and reduce the disputes between the parties after seeing the parties' P.R. 4-3 filings, VirnetX has explicitly required that a "domain name" is "to be sent to a domain name service (DNS)."

computer or group of computers," when it describes that the IP address corresponding to the destination computer "need not be the actual IP address of the destination computer." *Id.* at 38:23-42. In other words, an IP address that corresponds to the domain name may not be the actual IP address of the destination computer, but rather an IP address corresponding to one of a group of computers which may be used to communicate with the destination computer. The extrinsic evidence is consistent with VirnetX's construction that a domain name may correspond to a "group of computers," such as a network. *See Ex.* 17 at 172 ("An alphanumeric string which identifies a particular computer *or a network on the Internet.*") (emphasis added).

Microsoft's Proposed Construction. Microsoft's proposed construction that the domain name must be in a "hierarchical" format is another attempt to limit the claims to DNS as extrinsically implemented by the IETF. No form of the word "hierarchical" is found in the patent. Microsoft's "hierarchical" limitation is contrary to the specification's description of a modified form of DNS handling domain name requests that may not be hierarchical, *e.g.*, domain name extensions. *'135 patent* at 38:23-33. The word "hierarchical" in RFCs 1034 and 1035, on which Microsoft relies, describes the name space, not the names themselves. *Ex.* 15 at 1, 50; *Ex.* 16 at 49; *Ex.* 4 (*Jones Decl.*) ¶23. Microsoft's construction thus raises the question, what is "hierarchical," and by contrast, what is not "hierarchical," as far domain names are concerned?

Moreover, Microsoft's proposed construction ignores the specification and imports unwarranted limitations into the claim by limiting the domain name to a particular computer providing web pages on the World Wide Web ("such as www.utexas.edu"), despite no limiting lexicography, disclaimer or disavowal. *See Voda v. Cordis Corp.*, 536 F.3d 1311, 1320 (Fed. Cir. 2008) (The Federal Circuit has "cautioned against importing limitations from the specification into the claims.") (citing *Phillips*, 415 F.3d at 1323).[6] World Wide Web sites providing web pages over the Internet are not the only computers with domain names. *Ex.* 4 (*Jones Decl.*) ¶25. The intrinsic evidence's definition of a

[6] Microsoft's "such as www.utexas.edu" limitation is also improper as merely exemplary. The jury is left to guess as what is meant by "such as." Does it have to be domain names of the type on the World Wide Web for educational institutions with the domain ".edu?" This creates confusion for the jury.

VPN as carrying "traffic" indicates it is not limited to carrying web pages; other applications can be used.

Furthermore, Microsoft's construction erroneously excludes the preferred embodiment. *See Vitronics Corp. v. Conceptronic*, 90 F.3d 1576, 1583 (Fed. Cir. 1996) (a claim interpretation that excludes a preferred embodiment is "rarely, if ever, correct"). In the preferred embodiment of the '135 patent, "address hopping" is used. *'135 patent* at 38:1-6. As the patent specification declares for this preferred embodiment, "[e]xamples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like." *Id.* at 19:42:44. None of these examples from the patent are web pages. A web browser requesting web pages is merely an "example" of an application that can be used. *Id.* at 37:30-39. Further intrinsic evidence in the form of a cited reference makes it apparent that a VPN can "handle new software applications without disturbing the existing private data network," further indicating that the VPN, and domain names, are not limited to World Wide Web sites providing web pages. *See Ex.* 10 (VNET 00221857).

Microsoft's proposed limitation that the domain name is a name that the DNS "converts into an IP address" conflicts with the specification. The IP address of the destination computer may not be returned, but instead the message "host unknown" may be returned. *'135 patent* at 38:43-52; 39:21-25; 39:53-60. Moreover, the DNS may not do anything with the domain name or DNS request. As described in the preferred embodiment, a DNS proxy or modified DNS may respond to the DNS request. *Id.* at 38:23-39:41.

VirnetX's proposed construction of the term "domain name" gives due breadth to the claim language, whereas Microsoft's proposed construction imports unwarranted limitations into the term. VirnetX's construction should be adopted.

E. secure web site

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a computer associated with a domain name and that can communicate in a virtual private network	web site that requires authorization for access ************************************ a "web site" is "one or more related web pages at a location on the World Wide Web"

The dispute about the construction of the claim term "secure web site" is whether the term is a computer capable of hosting varied applications and protocols, as is described in the '135 patent, or whether the term should be limited to one application, web pages, one protocol, HTTP, all on the World Wide Web, as proposed by Microsoft. The intrinsic evidence favors VirnetX's proposed construction.

VirnetX's Proposed Construction. Nowhere do the '135 patent claims recite the term "web site" by itself. The disputed term at issue is "secure web site." VirnetX has properly focused on the entire term. The term "secure" (and therefore "secure web site") is a term that does not have a single ordinary meaning in the art and must be understood by reference to the intrinsic evidence.

The claim language itself is instructive and supports VirnetX's proposed construction that a "secure web site" is a computer "that can communicate in a virtual private network." Each of claims 1 and 10 is directed to a method or system of "transparently creating [create] a virtual private network (VPN) between a client computer and a target computer." The target computer, with which VPN communications are trying to be established, corresponds with the "secure web site." In creating the VPN, claim 1 recites in step (2) "determining whether the DNS request transmitted in step (1) is requesting access to a secure web site," and if access to a secure web site is requested, step (3) recites "…automatically initiating the VPN between the client computer and the target computer." Similarly, claim 10 requires a DNS proxy server that "generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested." The claim language itself thus associates the "secure web site" with a computer that can communicate in a VPN (*e.g.*, the secure target computer), as proposed by VirnetX.

The specification describes a "secure web site" as a computer that can communicate in a VPN. The specification describes a "secure web site" as a "secure target site" 2604 in Figure 26:

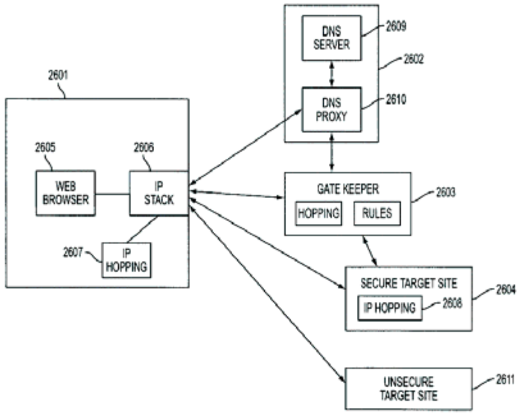


FIG. 26

'*135 patent* at 38:23-42; Fig. 26. The specification also describes a "non-secure web site 2611," as an "unsecure target site" 2611 in Figure 26. *Id.* at 38:43-52; Fig. 26.

Importantly, in distinguishing a secure web site from a non-secure web site, the specification describes the "secure web site" (associated with a secure target site 2604) as a secure "host" that is "equipped with a secure communication function such as an IP hopping function 2608." *Id.* at 38:53-60; *see also id.* at 38:66-39:25 (describing "secure host").[7] (Similarly, the patent describes a "web site" as a "host," at column 37, lines 30-39.) There are three aspects of the description of a "secure web site" that are important here. First, it has a "secure communication function." Secure communication is provided in the context of the invention through encryption in a VPN. *Id.* at 1:38-45; 6:1-3; 19:66-20:3. Second, the use of the term "secure host" to describe the "secure web site" reflects its nature as any computer capable of being connected to and communicating in a VPN using any application, and need not provide web pages in response to web browser requests.[8] Third, the secure web site is a secure host with a secure communication function "such as an IP hopping function." In the preferred

[7] The secure communication function of the IP hopping function in the preferred embodiment is one way of implementing a VPN. *See* '135 patent at 38:2-6.

[8] *Ex.* 12 at 231 ("TCP/IP defines the term host computer to refer to any computer system that connects to an internet and runs applications."); *Ex.* 12 at 527 ("Host: An end-user's computer connected to a network. In an internet, each computer is classified as a host or a router."); *Ex.* 18 at 11 ("A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e. application) programs. We will follow the traditional usage and call these machines hosts.").

embodiment of the '135 patent, IP address "hopping" is used, and the specification explicitly states for this embodiment that "[e]xamples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like." *Id.* at 38:1-6; 19:42:44. Web pages are not required.

The specification's description of a secure web site as a secure host, which may host various applications, is consistent with other parts of the specification. The specification states a web browser requesting web pages is merely an "example" of a conventional client application. *Id.* at 37:30-32 ("This conventional scheme is shown in FIG. 25. A user's computer 2501 includes a client application 2504 (for example, a web browser) and an IP protocol stack 2505 … "); 38:14-16 ("A user's computer 2601 includes a conventional client (*e.g.*, a web browser) 2605 …"); *accord id.* at 37:22-29. For Microsoft's construction to be adopted the specification language "for example" and "e.g." must be ignored.

As part of the intrinsic evidence, the prosecution history is consistent with the specification, reflecting the Examiner's view that the secure target computer (associated with a secure web site) is a "secure host." *See Ex.* 19 (Paper No. 13), p. 1 (VNET00221503). Consistent with the specification, the Examiner thus viewed the term "secure web site," as a secure host -- any computer capable of being connected to and communicating in a VPN, and not necessarily only providing web pages.

Nor is there any aspect of the inventions described in the patents that makes them uniquely applicable to web pages or the http protocol on the World Wide Web. The specification distinguishes the prior art on the basis of the invention's creation of VPNs between a client computer and a target computer in response to a DNS look-up function. *'135 patent* at 37:17-21. This capability in the invention is not dependent on the kind of application being used (*e.g.*, e-mail, word processing programs, telephony, web pages etc.). A problem of the prior art was that VPNs were not easy to establish. This problem, like the solution of the '135 patent, is unrelated to the type of traffic that will ultimately use the VPN.

The specification also supports VirnetX's proposed construction that a "secure web site" is "associated with a domain name." As described in the specification, the DNS request for the secure target computer may not return the actual IP address of the secure target computer. *Id.* at 38:36-42. As discussed above for the claim term "domain name," an IP address that corresponds to the domain name may not be the actual IP address of the destination computer. For example, a DNS request may resolve to a single IP address, but be associated with multiple computers. Similarly, as described above in the specification, a DNS request for a "secure web site" may resolve to a single IP address, but be associated with one computer or more computers. *Id.* Thus, VirnetX's proposed construction that a "secure web site" is "associated with a domain name" is firmly supported by the specification.

Microsoft's Proposed Construction. Microsoft has focused only on the term "web site" rather than the entire claim term "secure web site," and has reached an improper construction. The Federal Circuit has emphasized the need to construe the entire claim term, and Microsoft's isolation of the words "web site" from the word "secure," flouts the Federal Circuit's instruction. *See Warner-Lambert Co. v. Purepac Pharm. Co.*, 503 F.3d 1254, 1264 (Fed. Cir. 2007) (" … the construction adopted by the district court gives full meaning to every word of the entire claim term …").

Further, Microsoft's proposed construction of "one or more related Web pages at a location on the World Wide Web" invites error. In construing "secure web site," the Court must focus "at the outset on how the patentee used the claim term in the claims, specification, and prosecution history." *Phillips*, 415 F.3d at 1313. The *Phillips* approach establishes the correctness of VirnetX's proposed construction and the failings of Microsoft's alternative. Microsoft's proposed construction is based on its selective use of self-serving extrinsic dictionary definitions and extrinsic expert testimony regarding the partial term "web site." *JCC Exh. E* ¶17. Microsoft offers no dictionary definition for the entire term "secure web site" because there is none. *Id.*

Microsoft's unduly narrow limitations of the specific application of "Web pages" and "the World Wide Web" finds no support in the claim language. There is no limitation in the claims as to what particular application or protocol is transmitted over the resulting VPN. There is no mention of the "World Wide Web," "web pages," or a "web browser" in the claims. Instead, the claims were written to support the use of any application for secure communication between a client computer and a target computer using a VPN, which carries "traffic," not limited to any particular application or network. As the specification explicitly calls out, a web browser requesting web pages is merely one example of a conventional client application. *'135 patent* at 37:30-39; 38:14-16. The web browser example in the specification was used to demonstrate merely one application in the prior art (as shown in Figure 25), and the invention is not limited to this one application of the prior art: there is no limiting lexicography, disclaimer or disavowal.

Microsoft argues that the specification describes both the prior art (depicted in Figure 25) and the invention (an embodiment of which is in Figure 26) as using a web browser (2504 or 2605) *JCC Exh. E* ¶18. The claim language does not mention a "web browser", so Microsoft's reliance on a web browser is misplaced. Moreover, unlike the one example of an application in the conventional scheme described and depicted in Figure 25, in describing the Figure 26 embodiment of the invention, the specification does not limit the secure web site to providing web pages in response to a web browser making page requests on the World Wide Web. *'135 patent* at 38:13-65; Fig. 26. The target site 2604 in Figure 26 is labeled "secure," and there is no indication in the embodiment of Figure 26 that the requests made to the "secure" target site are web page requests, or that the secure target site must provide web page responses. *Id.* In fact, as discussed above, in the preferred embodiment, other applications can be used; it does not have to be web pages. *Id.* at 38:1-6; 19:42-44. Nor is there any indication that the Examiner viewed the invention as requiring the secure web site to implement the specific application of providing web pages in response to a web browser's request for web pages on the World Wide Web.

Finally, Microsoft's proposal of web pages at World Wide Web location "that requires authorization for access" finds no support in the intrinsic evidence of what it means to be a "secure" web site, limits the claims to a preferred embodiment, and violates claim differentiation. Security, in the context of the invention, is about encryption in a VPN, not authorization *per se*. *'135 patent* at 1:38-45; 19:66-20:3. Microsoft acknowledges that "[t]he patents-in-suit describe 'data security' as 'usually' being tackled using some form of data encryption." *JCC Exh. E* ¶54. Moreover, although authorization is described in the specification, this is merely in a preferred embodiment of the invention. *'135 patent* at 38:66-39:25. Such authorization is separately claimed in dependent claims 4, 5, 9, and 12, which strongly counsel against so limiting the terms in independent claims 1 and 10.

Microsoft's argument that VirnetX's construction does not make the secure web site truly "secure" is a red herring. *JCC Exh. E* ¶22. VirnetX's construction limits the secure web site to a computer that "can communicate in a VPN."

This dispute about the term "secure web site" should be resolved in favor of VirnetX's construction over Microsoft's since VirnetX's constructions is firmly grounded in the intrinsic evidence. In contrast, Microsoft's construction erroneously relies on inconclusive extrinsic dictionary definitions, and tries to limit the claims to one particular application, contrary to the intrinsic evidence.

"*Web site*." Microsoft offers no good reason to isolate the words "web site" and construe them alone. They are never found alone in the claims. However, to the extent the Court wants to separately construe the words "web site," they should be construed as "a computer associated with a domain name and that can communicate in a network." The specification supports VirnetX's proposed construction. In the patent, the inventors used the term "web site" as a short-hand reference to a computer associated with a domain name in a network. In the Background section of the patent, the specification equates a "web site" with a "destination terminal," shown as 110 in Figure 1. *'135 patent* at 1:15-37; Fig. 1. As indicated above, a "web site" is a particular kind of "Internet resource," one with an associated domain name. *Id.* at 1:34; 37:19-29. Not all Internet resources are so associated. *Ex.* 4 (*Jones Decl.*) ¶25 (not all computers on the Internet have domain names); *Ex.* 28 (Johnson Depo. Tr.) at 244-245 (same). Consistent with the specification's description of a "secure web site," the specification equates the term "web site" with a "host." This is evident in the specification's description of the conventional scheme, in which a target web site 2503 is identified as a "host." *'135 patent* at 37:30-39; Fig. 25. As discussed above, the use of the term "host" to describe the "web site" reflects its nature as any computer capable of being connected to and communicating in a network using any application, and need not provide web pages in response to web browser requests. A web browser requesting web pages is merely an "example" of a conventional client application. *Id.* at 37:30-32; 38:14-16; *see also id.* at 19:42:44.

F. determining whether the DNS request transmitted in step (1) is requesting access to a secure web site

VirnetX's Proposed Construction	Microsoft's Proposed Construction
No further construction required. To the extent the Court construes the phrase: determining whether the DNS request transmitted in step (1) is requesting VPN communication with a secure web site	the computer receiving the DNS request checks the request to determine whether access to a secure web site was requested

The dispute about the claim phrase "determining …" (for short) in claim 1 of the '135 patent is whether this phrase requires any construction at all beyond the terms already construed, namely, "DNS" and "secure web site," as proposed by VirnetX, or whether the additional claim language requires construction, as proposed by Microsoft, and if so, what further construction. The additional claim language uses ordinary language that the jury can understand so no further construction is required. Microsoft's construction imports unwarranted limitations into the phrase.

VirnetX's Proposed Construction. The DNS request transmitted in step (1) is the DNS request that was generated as result of the step of "generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer." So the claim itself says what the DNS request is, a request that requests an IP address corresponding to a domain name associated with the target computer. The Court has also been asked to separately construe the terms "DNS" and "secure web site." The rest of the claim language in the disputed "determining …" phrase is, as italicized, "*determining whether the* DNS request transmitted in step (1) *is requesting access to* a secure web site." These terms will be familiar to the jury and need no further construction. Not every claim term or phrase requires construction. *See U.S. Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997).

To the extent this Court determines any construction is necessary, the specification supports VirnetX's alternative proposed construction of (with additional construction italicized) "determining whether the DNS request transmitted in step (1) is requesting *VPN communication with* a secure web site." When a client computer generates a DNS request to access a secure web site, it is seeking VPN communication with the site. *'135 patent* at 37:63-38:2. In response to a DNS request for a secure web site, a VPN is set up. *Id.* at 38:23-42. *See also id.* at 38:53-60; 39:21-33 (same). When the client computer seeks to access the secure web site, it is seeking to connect to the site through a VPN. *Id.* at 39:7-9; *see also id.* at 39:2-6 (if access to a secure site is not requested, no VPN is created); 39:21-25; 39:42-52 (if access to a secure site is requested, a VPN is created).

Microsoft's Proposed Construction. As discussed above, Microsoft's definitions of "DNS" (requiring the IETF DNS) and "secure web site" (requiring provision of web pages on the World Wide Web) are flawed, so too is its definition of this "determining …" phrase in step 2 of claim 1 that includes those terms.

Moreover, Microsoft's proposal of "the computer receiving the DNS request checks the request" is an attempt to limit this *method* claim to the particular network architecture of the preferred embodiment. Microsoft argues that the "determining" step cannot be performed by the client computer. *JCC Exh. E* ¶25. There is no such structural limitation in method claim 1. There is nothing in the claim language that says what does the "determining" step and checks the DNS request, and there is no basis to import a limitation from the preferred embodiment into the claim. *See Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1303 (Fed. Cir. 2007) ("This court has cautioned against limiting the claimed invention to preferred embodiments or specific examples in the specification."). Microsoft is actually trying to rewrite claim 1 by taking the transmitted DNS request (from step (1)) and replacing it with a computer that has received the request. There is nothing to say that the transmitted DNS request could not be determined (as in step (2)) by the transmitting computer (or a receiving computer). Microsoft is simply trying to impose structural limitations on where the claimed functions occur in an effort to avoid infringement. There is no basis for importing into the claim language any limitations on where the claimed function is carried out, and certainly no basis to exclude the client computer from performing the claimed function.

Claim differentiation also counsels against Microsoft's construction. Claim 2, which depends on claim 1, recites "The method of claim 1, wherein steps (2) and (3) are performed at a DNS server separate from the client computer." Step (2) is the "determining" step. So dependent claim 2 demonstrates that the "determining" step in claim 1 can happen at a DNS server on the client computer.

Microsoft's objection that VirnetX is seeking "to replace the claim term 'requesting access' with 'requesting VPN communication'" is misplaced. *JCC Exh. E* ¶28. VirnetX does not believe the claim language requires further construction. But, to any extent that it does, the patent describes that a request for access to a secure web site is a request for VPN communication with that site. *'135 patent* at 37:63-38:2; 38:23-33. Microsoft's argument that the DNS request itself does not request a VPN is inconsistent with the claim language of determining whether the DNS request transmitted in step (1) is "requesting access to a secure web site," and if so, "automatically initiating the VPN."

This claim phrase requires no construction, but if it is construed, it should be construed as proposed by VirnetX since only VirnetX's construction is supported by the specification but without limiting the claim to the preferred embodiment.

G. automatically initiating the VPN

VirnetX's Proposed Construction	Microsoft's Proposed Construction
starting the VPN without intervention by a person	initiating the VPN without the client or target computer requesting such initiation

The dispute about this term in claim 1 of the '135 is whether the term indicates a VPN is to be started without intervention by a person, as proposed by VirnetX, or without particular computers requesting the initiation of a VPN, as proposed by Microsoft. The overwhelming evidence shows that the word "automatically" (in contrast to manually) in this context means the VPN is started without intervention by a person. Thus, VirnetX's proposed construction is correct.

VirnetX's Proposed Construction. The claim language supports VirnetX's construction. The claim says "in response to determining that the DNS request in step (2) is requesting access to a secure web site, automatically initiating the VPN between the client computer and the target computer." The body of the claim thus emphasizes that rather than a person starting the VPN, the VPN is started by a machine. However, as the claim language indicates, there is no limitation as to which particular machine starts the VPN. According to the claimed invention, it does not matter which machine starts the VPN. In contrast to the prior art, the important point is that the VPN is started without intervention by a person.

The specification also supports VirnetX's proposed construction. In describing the FreeS/WAN conventional scheme, the specification equates "automatically" with the idea of a user not entering information required for a VPN. The specification says this conventional scheme "allows hosts to ***retrieve automatically the public keys*** of a host that the host is to communicate with so that the host can ***set up a VPN without having the user enter the public key*** of the destination host. One implementation of this standard is presently being developed as part of the FreeS/WAN project (RFC 2535)." *'135 patent* at 37:53-58 (emphasis added). The specification does not distinguish the FreeS/WAN prior art on the basis of this automatic aspect. Rather, the specification says that, unlike this prior art, the invention "automatically sets up a virtual private network between the target node and the user" ***by looking at the DNS request***, and differentiating between DNS requests, so that different DNS requests yield different results. *Id.* at 37:59-38:2; 38:23-52. According to the specification, "[a] second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function." *Id.* at 37:19-21. Unlike the prior art, the DNS request triggers the VPN in the '135 patent.

The prosecution history is consistent. As part of the intrinsic evidence, cited references distinguish manual configuration by a person from automatic configuration by a machine – software, firmware or hardware. *Ex.* 20 at 13:52-55; *Ex.* 7 at 3:50-52; *Ex.* 21 at 1:50-54; *Ex.* 22 at 1 ("The software automatically notices each newly installed box, and doesn't require a network administrator to reconfigure it. Instead of 'virtual private networks' we have a 'REAL private network'; we add privacy to the real network instead of layering a manually-maintained virtual network on top of an insecure Internet."); *Ex.* 6 at 3 ("Automatic keying: A mode in which keys are automatically generated at connection establishment and new keys automatically created periodically thereafter. Contrast with manual keying in which a single stored key is used.").

Microsoft's Proposed Construction. Microsoft's construction precludes either the client computer or the target computer from requesting the starting of a VPN. As discussed above concerning the "transparently …" phrase, dependent claims such as claims 2 and 12 indicate that the client computer can be involved in creating the VPN. Microsoft's proposed construction is simply another attempt to limit the claim language to the preferred embodiment. *'135 patent* at 38:23-33. But, again, this all happens "[a]ccording to one embodiment," and is not a requirement of the language in method claim 1 of the '135 patent. *Id.*

Both the intrinsic and extrinsic evidence support VirnetX's proposed construction, and there is no lexicography, disclaimer, or disavowal to import a limitation from the preferred embodiment into the claim, as in Microsoft's proposed construction.

H. DNS proxy server

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a computer or program that responds to a domain name inquiry in place of a DNS	a computer that intercepts a DNS request from a client computer to a DNS server and checks the request to determine whether access to a secure web site has been requested

The dispute about the term "DNS proxy server" in claim 10 of the '135 patent is whether the term describes a computer or program that responds to a domain name inquiry in place of a DNS, as VirnetX proposes, or is limited to a separate computer interposed between a client computer and a DNS server, as in Microsoft's proposal. The intrinsic evidence shows that a "DNS proxy server" is either a computer or a program; this function need not be carried out on a separate computer interposed between a client and a DNS server.

VirnetX's Proposed Construction. The claim language supports VirnetX's proposed construction. The claim language says "a DNS proxy server that receives a request from the client computer to look up an IP address for a domain name." From this claim language, it is apparent that the DNS proxy server responds to a domain name inquiry. Further, the language "proxy" says that the DNS proxy server responds in place of a DNS.

The specification clearly describes the DNS proxy server as either a computer or a program, as in VirnetX's construction. The specification says that in the preferred embodiment, the DNS proxy server is a set of "functions," which can either be on a separate server, or combined with other functionality on a single server. *'135 patent* at 38:61-65. Further, the specification describes that the DNS proxy server responds to DNS requests in place of a DNS. For example, the specification says that the DNS proxy server responds to a "domain name inquiry." *Id.* at Abstract; 5:65-6:3; 32:29-35. "FIG. 27 shows steps that can be executed by DNS proxy server 2610 to handle requests for DNS look-up for secure hosts." *Id.* at 38:66-39:1. As a proxy, the DNS proxy server responds to DNS requests in place of a DNS server. *Id.* at 38:23-33; 38:43-52; 39:42-40:13.

The prosecution history is consistent. During prosecution, the inventors never made any concessions about the location of the DNS proxy server. Instead, in distinguishing the prior art, they emphasized its functionality: "[a]t a minimum, neither Boden nor Risley discloses a DNS proxy server that 'generates a request to create the VPN between the client computer and the secure target computer if it is determined that access to a secure web site has been requested …'" *Ex.* 9 at 6. Contrary to any limitation about the placement of the DNS proxy server, during prosecution, there were claims directed to "… a domain name server (DNS) proxy module that intercepts DNS requests sent by a client …" *Ex.* 23 at 1, 3, 4. However, these claims were canceled as a result of a restriction requirement by the Examiner. *Ex.* 19 at 1-3.

Microsoft's Proposed Construction. In addition to including its erroneous constructions of the terms "DNS" and "secure web site," Microsoft argues that the DNS proxy server includes a structural limitation that requires a separate computer interposed between the client computer and a "DNS server" and intercept a DNS request from the client computer to the DNS server. *JCC Exh. E* ¶43. To begin with, there is no "DNS server" recited in claim 10, and no good reason to read this into the claim. Nor is there any mention that the DNS proxy server "intercepts" a DNS request. Interpreting the word "receives" in the claim as "intercepts" would substantially alter the meaning of the word "receives." Further, claim differentiation suggests a broader scope. Although dependent on claim 1, claim 8 says "… a DNS proxy server that passes through the request to a DNS server if it is determined in step (3) that access is not being requested to a secure target web site." Unlike claim 8, there is no language in claim 10 that suggests that the DNS proxy server in claim 10 intercepts a DNS request to a DNS server.

Microsoft's proposal also suggests that the DNS proxy server functionality is not a program or part of a client computer, pointing to the description of an embodiment depicted in Figure 26. *JCC Exh. E* ¶46. Here again, claim differentiation indicates claim 10 is broader. Claim 2, which depends on claim 1, recites "a DNS server separate from the client computer." There is no such language in claim 10 suggesting that the DNS proxy server must be separate from the client computer. To further explain, claims 1 and 10 are method and system siblings. Claim 2 suggests that the steps of determining whether a DNS request is requesting access to a secure web site, and initiating the VPN for such a request, may take place at DNS server on the client computer in claim 1. As described in the patent, this DNS server performing this functionality may be a DNS proxy server. *'135 patent* at 37:17-21; 38:13-65. Claim 10 has no limitation as to where the DNS proxy server functionality is, like claim 1, and unlike claim 2. The physical location where the DNS proxy server functions are performed is not dictated by the nature of the invention or the claim language. *See '135 patent* at 38:61-65; *see also id.* at 38:53-60 ("Gatekeeper 2603 can be implemented on a separate computer (as shown in FIG. 26) or as a function within modified DNS server 2602.").

VirnetX's proposed construction of a DNS proxy server is the most natural reading of the claim language in view of the intrinsic evidence, whereas Microsoft's construction seeks to impose functional and architectural requirements that go way beyond the claim language, and which are inconsistent with the intrinsic evidence.

V. VIRNETX'S PROPOSED CONSTRUCTIONS FOR THE '759 PATENT CLAIM TERMS AND PHRASES SHOULD BE ADOPTED.

The '759 patent contains two independent claims, claims 1 and 16. Both claims contain the four disputed claim terms and phrases in the '759 patent, as indicated in bold and underlining below:

> 1. A method for establishing a **secure communication link** between a first computer and a second computer over a computer network, the method comprising steps of:
>
> **enabling a secure communication mode of communication at the first computer without a user entering any cryptographic information for establishing the secure communication mode of communication**; and
>
> establishing the secure communication link between the first computer and a second computer over a computer network based on the enabled secure communication mode

> of communication, **the secure communication link being a <u>virtual private network</u> communication link** over the computer network.
>
> * * * * * * * * * * *
>
> 16. A computer-readable storage medium, comprising: a storage area; and
>
> computer-readable instructions for a method for establishing a **secure communication link** between a first computer and a second computer over a computer network, the method comprising steps of:
>
> **enabling a secure communication mode of communication at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication**; and
>
> establishing a secure communication link between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication, the **secure communication link being a <u>virtual private network</u> communication link** over the computer network.

A. <u>virtual private network communication link</u>[9]

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a communication path between computers in a virtual private network	communication link in a virtual private network

In addition to the disputed construction of the embedded term "virtual private network" (discussed above),[10] the disputed construction of the claim phrase "virtual private network communication link" is whether the phrase is the entire communication path between computers in a VPN, as proposed by VirnetX. The intrinsic evidence supports VirnetX's construction. Microsoft merely rearranges the words in the claim while offering no construction for the word "link."

VirnetX's Proposed Construction. The claim language says "establishing a secure communication link between the first computer and a second computer over a computer network …, the secure communication link being a virtual private network communication link over the computer network." The claim language thus says that the VPN communication link is a secure "communication link" that is "over the computer network." This language supports VirnetX's proposed construction that the VPN communication link is the entire communication path between computers in a VPN.

[9] The parties agree that the term "virtual private network communication link" should be construed consistently in both the '759 and '180 patents, where it is found.

[10] The parties agree that the term "virtual private network (VPN)" should be construed consistently in all three patents.

The specification is consistent and supports VirnetX's proposed construction. It describes the VPN communication link as a secure "communication" link between computers "over a [the] computer network," beginning with the Abstract, and continuing with the Summary of the Invention and the rest of the specification. *'759 patent* at Abstract; 6:63-65; 50:50-64; 51:45-47; 53:38-42; 53:48-55.

Microsoft's Proposed Construction. Microsoft's proposal is merely a rearrangement of the words in the disputed term without defining the word "link," and thus is not helpful to the jury. The specification makes it clear that not all links are VPN links. *'135 patent* at 36:25-32; *see also id.* at 52:12-29. Microsoft's proposal fails to take account of important claim language, namely that the link here is a VPN "communication" link "over the computer network." A VPN "communication" link that is "over the computer network" must include the entire path between the two computers.

The intrinsic evidence overwhelmingly supports VirnetX's proposed construction and trumps Microsoft's proposal, which is no real construction at all.

B. secure communication link (… the secure communication link being a virtual private network communication link)

VirnetX's Proposed Construction	Microsoft's Proposed Construction
virtual private network communication link	encrypted communication link

The dispute between the parties is whether the claim itself defines a "secure communication link" as a "virtual private network communication link" such that it requires no further construction, as proposed by VirnetX.

VirnetX's Proposed Construction. The claims specifically recite "the secure communication link being a virtual private network communication link." Like the claims, the specification also says "[t]he secure communication link is a virtual private network communication link over the computer network." *'759 patent* at 6:63-65. "Secure communications" are according to the inventive principles of the patent, and those principles are limited to VPNs. *See id.*; *also see id.* at 22:14-19. During prosecution, the Examiner emphasized this in his Statement of Reasons for Allowance: "The prior arts [sic] of record do not teach a system and a method for establishing a secure communication link being a virtual private network communication link between a client computer and a server computer over a computer network." *Ex.* 24 at 2. The Title of the '759 patent is, after all, "Method for establishing secure communication link between computers of virtual private network without user entering any cryptographic information." A secure communication link is thus a virtual private network communication link, which has already been construed. No further construction is required. *See U.S. Surgical*, 103 F.3d at 1568.

Microsoft's Proposed Construction. Microsoft proposes that a secure communication link is an encrypted communication link. However, as discussed above, not all encrypted communication links are VPN communication links. *'759 patent* at 38:65-39:4. Security in the context of the patent is not merely about encryption, it is about encryption in a VPN. *Id.* at 1:49-56. Moreover, the claims say that a secure communication link is between a first computer and a second computer "over a computer network." This claim language itself indicates that the secure communication link is in a network. Microsoft's proposal fails to account for this. In contrast, VirnetX's proposal properly recognizes this claim language by saying that the secure communication link is a "virtual private network" communication link. Microsoft's argument that under VirnetX's proposal, "one can argue that any 'secure communication link' is a VPN" (*JCC Exh. E* ¶55) completely ignores VirnetX's construction that the secure communication link *in the claims* is a "virtual private network communication link."

VirnetX's proposal is superior to Microsoft's because it defines the term as the claim language itself defines the term.

C. enabling a secure communication mode of communication at the [a] first computer without a user entering any cryptographic information for establishing the secure communication mode of communication

VirnetX's Proposed Construction	Microsoft's Proposed Construction
providing to the first computer at least one resource necessary for a virtual private network communication, based on a domain name service (DNS) that provides the resource according to user identity, without user input of encoding or decoding information	no construction necessary. In the alternative, to the extent the Court determines that a construction is needed for "cryptographic information," it is "information used for encryption"

The dispute about the construction of the claim phrase "enabling …" (for short) is whether the phrase requires reference to the '759 patent's specification to arrive at its meaning to the ordinarily skilled artisan, as proposed by VirnetX, or whether the phrase requires no construction at all, as proposed by Microsoft. The claim language in this entire phrase cannot be understood without reference to the intrinsic evidence and thus favors VirnetX's proposed construction. Whereas Microsoft's proposed construction fails to provide any clarity as to what is meant by "enabling" or "establishing" a "secure communication mode of communication" without a user entering cryptographic information.

VirnetX's Proposed Construction. The disputed phrase is an instance where the specification provides clarity to the claim language by disclaiming the prior art conventional scheme and specifically defining the invention. *See Alcatel United States Res.*, 2008 U.S. Dist. LEXIS 49615, at *6. As the parties' experts agree, the ordinarily skilled artisan would look to the specification to determine what a "secure communication mode of communication" is, and how it is enabled without a user entering "cryptographic information" for establishing the mode. *Ex.* 4 (*Jones Decl.*) ¶34; *Ex.* 28 (Johnson Depo. Tr.) at 208-216. There are two key and connected aspects to the disputed phrase. The first is "enabling a secure communication mode of communication at the [a] first computer." The second is "without a user entering any cryptographic information for establishing the secure communication mode of communication." Both aspects share the phrase "secure communication mode of communication." The claim element by itself does not conclusively tell the ordinarily skilled artisan how a "secure communication mode of communication" can be enabled without the user entering "cryptographic information" for establishing the secure communication mode of communication. *Id.* The claim language does say in the second element of the claim "the secure communication link being a virtual private network communication link over the computer network." However, while the claim language itself says the secure communication mode of communication is enabled without a user entering "cryptographic information," it does not tell the ordinarily skilled artisan how this is done. The claim language thus invites reference to the specification for construction. The claim language, when interpreted in light of the specification, leads to only one construction, VirnetX's construction.

The Summary of the Invention section equates establishing a VPN with establishing a "secure communication mode of communication." *'759 patent* at 6:37-51. The Summary says that a VPN can be established without a user entering "user identification information, a password and/or an encryption key" for establishing the VPN. *Id.* at 6:37-41; *see also id.* at 51:34-41 (same). As seen above, the Summary then goes on to say that "[i]n one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication." *Id.* at 6:44-49. This embodiment corresponds to what is being claimed in claims 1 and 16. This portion of the specification describes enabling a secure communication mode of communication without a user entering cryptographic information for establishing the mode (as in claims 1 and 16) as a specific embodiment (*i.e.*, a species) of a user establishing a VPN without a user entering information such as an encryption key for establishing the VPN (*i.e.*, the genus).

Still unanswered by the Summary, however, is how the species claimed in claims 1 and 16 of the '759 patent enables a "secure" communication mode of communication "without a user entering cryptographic information." The rest of the specification answers this question. The specification first distinguishes the conventional scheme as having certain drawbacks even though a user can establish a VPN without entering encryption keys, a specific type of cryptographic information. *'759 patent* at 40:24-37. Specifically, the conventional scheme includes a DNS server that provides the encryption keys so that a VPN can be established without the user entering the keys. *Id.* However, this conventional scheme has drawbacks, particularly that "any user can perform a DNS request," which is a significant drawback because it fails to authenticate the requestor before enabling the VPN. *Id.*

The specification describes the invention as overcoming this problem, in a manner disclaiming the conventional scheme and defining the invention in a specific embodiment. The specification describes, in the conventional manner, a DNS may provide the cryptographic information (*e.g.*, public keys) for a VPN. *Id.* at 40:24-33. According to aspects of the invention, the specification goes on to describe a specialized DNS (domain name service) server that enables the VPN according to user identity, *i.e.*, "one for which secure communication services are defined." *Id.* at 40:37-44; *see also* 41:43-42:10; Fig. 27. The invention "automatically sets up a virtual private network" using a DNS for the authorized user so that the user does not have to enter cryptographic information. *See id.* at 40:37-44. On the other hand, the VPN is not enabled for users for which secure communications are not defined (*e.g.*, unregistered). *Id.* at 40:48-53. Thus, "[d]ifferent users who make an identical DNS request could be provided with different results." *Id.* at 40:54-55. This ability to differentiate DNS requests from different users distinguishes the invention from the described conventional scheme. *Id.* at 40:33-37. As described in the specification, if the user lacked credentials to establish a VPN connection, the specialized DNS server would deny the connection and return the message "host unknown" to the requestor. *Id.* at 41:23-28. Only those requestors who have a sufficient level of security can establish a VPN connection. *Id.* at 41:51-64; 41:65-42:2; 42:19-38. Thus, as described in the specification, a "secure communication mode of communication" or VPN communication is enabled based on a domain name service according to user identity, as proposed by VirnetX. Put another way, the VPN is enabled only for certain users.

What remains are (1) what the claims mean when they say "enabling" a secure communication mode of communication, a VPN communication mode, *i.e.*, what is necessary for a VPN communication, and (2) what "cryptographic information" is since the claims require "without the user entering cryptographic information." First, the specification describes a "VPN resource" (*e.g.*, encryption keys) as necessary for VPN communication. *See '759 patent* at 53:17-19; *see also id.* at 51:34-44 (describing provision of encryption keys transparently to the user, or without the user needing to be involved). Second, "cryptographic information" is encoding or decoding information. *Id.*; *Ex.* 25 at 280 ("Cryptography: the enciphering and deciphering of messages in secret code or cipher."). Putting it all together, the "enabling …" step requires "providing to the first computer at least one resource necessary for a virtual private network communication, based on a domain name service (DNS) that provides the resource according to user identity, without user input of encoding or decoding information," as proposed by VirnetX.

Microsoft's Proposed Construction. Microsoft offers no real construction for the "enabling …" step other than "cryptographic information." Microsoft's proposal does not provide the jury with any guidance for "enabling a secure communication mode of communication at [a] the first computer" or "establishing the secure communication mode of communication." Microsoft's main objection to VirnetX's proposal is that the concept of DNS acting on a user's identity is not explicitly recited in the '759 patent claims. *JCC Exh. E* ¶49. However, as discussed above, as both parties' experts admit, the language cannot be conclusively understood by the ordinarily skilled artisan without reference to the specification. The claim does not recite the source of the cryptographic information but merely recites that the user is not the source. Microsoft's proposed construction does not answer this question raised by the claim language, and attempts to broaden claims 1 and 16 to read them on the prior art conventional scheme described in the patent specification itself. *JCC Exh. E* ¶51 ("on its face, this discussion of FreeS/WAN and DNSSEC means that the claims of the '759 patent are almost certainly invalid"). Given the nature of the claim language, which raises the question of how the "enabling …" is actually carried out without a user entering cryptographic information, it is proper to look to the specification to see how the claimed step is carried out in a way that is distinct from the described prior art conventional scheme. *See Phillips*, 415 F.3d at 1327 ("we have looked to whether it is reasonable to infer that the PTO would not have issued an invalid patent, and that the ambiguity in the claim language should therefore be resolved in a manner that would preserve the patent's validity.").

Microsoft's argument that "providing to the first computer at least one resource necessary for a virtual private network communication" is imprecise is unfounded. *JCC Exh. E* ¶49. There are claims in the patents in suit that include VPN resources. *'135 patent* claims 7 and 10. The '759 patent also describes VPN resources. *'759 patent* at 53:18-20.

Finally, Microsoft argues that "cryptographic information" is "information used in encryption." Microsoft's proposal rearranges the words in the claims, with defining them. Further, Microsoft's proposal only accounts for the encryption side, not the decryption side of VPN communications. What does "information used in encryption" mean? In contrast to Microsoft's ambiguous construction, VirnetX's proposal of "encoding or decoding information" provides clear guidance to the jury.

Microsoft's objections to VirnetX's proposal of "encoding or decoding information" are not well-founded. In the context of the rest of VirnetX's construction, it is clear that the "encoding or decoding information" is for the VPN, thus tying the encoding or decoding information to a cryptographic technique.

The "enabling …" step must be understood by the ordinarily skilled artisan with reference to the specification. The specification provides clarity. The specification disclaims the conventional scheme and describes the claimed invention. VirnetX's proposed construction properly takes account of this intrinsic evidence, whereas Microsoft's does not.

VI. VIRNETX'S PROPOSED CONSTRUCTIONS FOR THE '180 PATENT CLAIM TERMS AND PHRASES SHOULD BE ADOPTED.

The '180 patent contains three independent claims, claims 1, 17 and 33. All three claims contain the four disputed claim terms and phrases in the '180 patent, in bold and underlining below:

> 1. A method for accessing a secure computer network address, comprising steps of:
>
> receiving a **secure domain name**;
>
> sending a query message to a **secure domain name service**, the query message requesting from the secure domain name service a **secure computer network address** corresponding to the secure domain name;
>
> receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and
>
> sending an access request message to the secure computer network address using a **<u>virtual private network</u> communication link**.

* * * * * * * * * * *

17. A computer-readable storage medium, comprising:

a storage area; and

computer-readable instructions for a method for accessing a secure computer network address, the method comprising steps of:

receiving a **secure domain name**;

sending a query message to a **secure domain name service**, the query message requesting from the domain name service a **secure computer network address** corresponding to the secure domain name;

receiving from the domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a **virtual private network communication link**.

* * * * * * * * * * *

33. A data processing apparatus, comprising:

a processor, and

memory storing computer executable instructions which, when executed by the processor, cause the apparatus to perform a method for accessing a secure computer network address, said method comprising steps of:

receiving a **secure domain name**;

sending a query message to a **secure domain name service**, the query message requesting from the secure domain name service a **secure computer network address** corresponding to the secure domain name;

receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name; and

sending an access request message to the secure computer network address using a **virtual private network communication link**.

A. secure computer network address

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a network address associated with a computer capable of virtual private network communications	a network address that requires authorization for access

The dispute about the construction of the claim term "secure computer network address" is whether the term is a network address of a computer capable of VPN communications, as proposed by VirnetX, or whether the network address must be of a computer that "requires authorization for access," as proposed by Microsoft. There is nothing in the claim language or the other intrinsic evidence that limits the term to be a computer that requires authorization for access.

VirnetX's Proposed Construction. The claim language supports VirnetX's proposed construction. The claims say "sending an access request message to the secure computer network address using a virtual private network communication link." So the computer at the secure computer network address is capable of VPN communications over a VPN communication link.

The specification is consistent with the claim language as well. The specification describes a computer at a secure computer network address in the form of, *e.g.*, a "secure" server 3320 as having "VPN communication link capability" since it "can only be accessed through a VPN communication link." *'180 patent* at 52:27-40; Fig. 33. A "secure" computer is a computer capable of VPN communications in the context of the patented invention because security is always described in the context of the invention as provided by encryption in a VPN. This can be seen in the exemplary portions of the specification identified above, as well as column 1, lines 50-57. The specification also supports VirnetX's proposed construction that the network address is "associated with" a computer capable of VPN communications. As discussed above, the specification describes that there may be multiple secure computer network addresses associated with a single secure domain name. *See '180 patent* at 52:22-26 (multiple addresses associated with secure domain name).

Microsoft's Proposed Construction. Microsoft's proposed limitation that the secure computer network address "requires authorization for access" finds no support in the intrinsic evidence. Nowhere is there any "authorization" limitation in the claims.

The specification also does not support Microsoft's unwarranted limitations. Microsoft mistakenly equates security in the claim term with authorization, rather than encryption. Rather, security in the context of the VirnetX patents is addressed by encryption in a VPN. *'180 patent* at 1:50-57. Microsoft concedes that data security in the patents requires encryption. *See JCC Exh. E* ¶54 ("The patents-in-suit describe 'data security' as 'usually' being tackled using some form of data encryption."); *id.* at 15 n.7 ("the use of the term 'usually' when talking about 'data security' does not mean that the term 'secure communication link' must be broad enough to allow for types of security other than encryption").

Moreover, Microsoft's proposed "authorization for access" construction is limited to a particular aspect of an embodiment. Microsoft relies on column 46, line 66 through column 50, line 1 describing Figure 33, and asserts that this diagram depicts the "present invention" as using a secure portal to authorize users to access the secure computer network address. *JCC Exh. E* ¶60. But Figure 33 is described for SDNS 3313, which is simply part of an embodiment for which the invention is "suitable for use." *'180 patent* at 9:30-32; *accord* 50:1. This is merely an embodiment of the invention. The claims have no such limitation of either a "secure portal" or "authorization." Nor is there any lexicography, disavowal or disclaimer that would limit the secure computer network addresses handled by the SDNS to authorization.

Claim differentiation also counsels against such an authorization limitation, as dependent claims 6, 22 and 37 specifically recite a "level of service" limitation. *See '180 patent* at 52:12-26 (describing "different priority level of access in a hierarchy of access levels" to a secure site). This indicates there is no such authorization or level of service limitation in the independent claims.

VirnetX's proposed construction should be adopted over Microsoft's because it is supported by the intrinsic evidence and gives due breadth to the claim term, unlike Microsoft's.

B. secure domain name

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a domain name which indicates that it is to be translated into a secure computer network address by a secure domain name service	a non-standard top-level domain name (such as .scom, .sgov. or .sorg) that corresponds to a secure computer network address

The dispute about the construction of the claim term "secure domain name" is whether the term admits of a broader construction than the detailed description of the preferred embodiment in the specification. VirnetX's proposed construction properly defines the term without importing unwarranted preferred embodiment limitations into it, unlike Microsoft's.

VirnetX's Proposed Construction. The claim language supports VirnetX's proposed construction. The claims say "… the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name." From this claim language, it is clear that the secure domain name has a corresponding secure computer network address, and that the secure domain name service (SDNS) can translate the secure domain name into the secure computer network address.

The specification also supports VirnetX's proposed construction that the secure domain "indicates that it is to be translated into a secure computer network address by a secure domain name service." In other words, there is something about the secure domain name itself that indicates to the SDNS that it must be resolved by the SDNS as the query for a secure domain name will be sent to the SDNS. '*180 patent* at 51:29-35. For example, secure domain name names may be identified by forming them with domain name extensions, such as "website.scom," which will be sent to the SDNS for resolution. *Id.* at 53:26-40; Fig. 35; *accord* 7:29-42. The specification thus supports VirnetX's proposed construction.

Microsoft's Proposed Construction. Microsoft argues that the specification describes the invention in terms of a "non-standard top-level domain name." There are several problems with this argument. First, and most importantly, the invention is what is claimed. The claim language does not contain the "non-standard top-level" limitation which Microsoft tries to import. Nor does the claim language contain the language "hierarchical" which Microsoft tries to import through its flawed definition of a "domain name" from the '135 patent.

Second, claim differentiation contradicts Microsoft's argument. Dependent claims 11, 27 and 41 explicitly recite that the secure domain name has a "top-level domain name," unlike the independent claims. *See Phillips*, 415 F.3d at 1314. And nowhere is there any explicit limitation that the secure domain name be a non-standard top-level domain name.[11]

Third, there is nothing in the specification or prosecution history that amounts to lexicography, disavowal or disclaimer which would necessarily require the secure domain name to be a "non-

[11] Microsoft's motivation for seeking to unduly limit the secure domain name in the claims to non-standard top-level domain names (such as .scom) is to try to exclude otherwise secure domain names merely because they do not have the specific format described in the preferred embodiment in the patent, such as peer names handled by Microsoft's PNRP. *Ex.* 14.

standard top-level" or "hierarchical" domain name. *Rambus Inc. v. Infineon Techs. Ag*, 318 F.3d 1081, 1094-95 (Fed. Cir. 2003) ("While clear language characterizing 'the present invention' may limit the ordinary meaning of claim terms, such language must be read in context of the entire specification and the prosecution history. Although the above references, taken alone, may suggest some limitation of 'bus' to a multiplexing bus, the remainder of the specification and prosecution history shows that Rambus did not clearly disclaim or disavow such claim scope in this case.").

The specification contains no description of a secure domain name as "hierarchical." Moreover, Microsoft points to column 7, lines 29-31, and column 51, lines 29-31 (*JCC Exh. E* ¶59), but these actually refute Microsoft's argument. These explicitly refer to both "secure," "top-level," and "non-standard" domain names, thus indicating the "secure" domain names are not necessarily always "top-level" or "non-standard."

Further, these portions of the specification merely describe SDNS in terms of the types of secure domain names it is capable of handling, without saying, in all cases, that secure domain names must take the form of "non-standard top-level" domain names. Nor is there anything especially significant about the secure domain name being a non-standard top-level domain name in the examples described in the specification. Microsoft argues that the secure domain names must be non-standard top-level domain names because otherwise they would be resolved by the conventional DNS, creating conflicts between conventional DNS and SDNS. *JCC Exh. E* ¶¶59, 61. A glaring problem with this argument is that it relies on Microsoft's erroneous dichotomy of "standard" versus "non-standard" domain names and "conventional" versus "non-conventional" DNS, none of which is necessary or appropriate in construing the claims. This argument by Microsoft is further support for why its definition of domain name and DNS are incorrect.

Fourth, Microsoft's construction is an attempt to limit the claims to the preferred embodiment. Although the specification describes examples of .scom, .sgov. or .sorg, there is no basis to limit the claims to this particular form of a secure domain name. These are merely examples. *'180 patent* at 53:37-40. The important point about a secure domain name is that it is capable of being identified and handled by a SDNS, as proposed by VirnetX, not its particular form.

Fifth, what is a "non-standard top-level" domain name? Does this mean not in an industry standard, like IETF RFCs? Microsoft's construction provides no guidance for the jury about what "standard" or "non-standard" domains names are, and invites further disputes about any such construction.[12] Similar to the problems with its "domain name" construction, Microsoft's construction is subject to the vagaries of an unspecified (and perhaps evolving) definition by a standards body, such as the IETF. And what is a "top-level" domain name? The words "top-level" do not, by themselves, say what the format of the name is. That is why dependent claims 11, 27 and 41 recite specific examples of such names.

Finally, Microsoft's construction of a "secure domain name" incorporating its "domain name" construction has several internal conflicts. Microsoft has construed a "domain name" as "hierarchical" using the example "www.texas.edu." Microsoft's "secure domain name" construction requires "a non-standard top-level domain name" using examples ".scom, .sgov, .sorg." There are many internal conflicts in Microsoft's construction: (a) a top-level domain name (under Microsoft's understanding) is not hierarchical; it is just one name; (b) the three examples of .scom, .sgov, .sorg are not hierarchical; (c) the non-standard top-level domain name (and these three examples) are not to be converted by the IETF DNS (per Microsoft's constructions). In addition, Microsoft's construction does not make sense for another reason. The examples in the specification, such as ".scom," are used to *form* secure domain names. *'180 patent* at 51:51-57. The examples such as ".scom" are not themselves secure domain names. For example, the specification describes "website.scom" as an "example" of a "secure domain name." *Id.* at 53:37-40. This entire example of a secure domain name is not itself a top-level name once it is formed as "website.scom." *Ex.* 4 (Jones Decl.) ¶40. This is consistent with the claim language. For example, dependent claim 27 recites "The computer-readable medium according to claim 17, wherein the secure domain name has a top-level domain name that includes one of .scom,

[12] Microsoft's further proposal of "(such as .scom, .sgov. or .sorg)" is not helpful, but rather creates more ambiguity, because it provides no bounds. What does it mean that the secure domain name must be "such as" .scom, .sgov or .sorg? Must the name be in the form of "com", "gov" or "org"?

.snet, .sorg, .sedu, .smil or .sgov." This claim says the secure domain name "has" a top-level domain name, not that the secure domain name "is" such a name.

VirnetX's proposed construction should be adopted because it properly defines the term "secure domain name" in a manner helpful to the jury and is supported by the intrinsic evidence, whereas Microsoft's seeks to import unwarranted limitations into the term and raises more questions than it answers, violating many canons of claim construction.

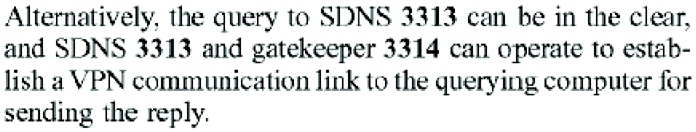
C. secure domain name service

VirnetX's Proposed Construction	Microsoft's Proposed Construction
a service that receives requests for secure computer network addresses corresponding to secure domain names, and is capable of providing trustworthy responses	a domain name service that provides secure computer network addresses for secure, nonstandard top-level domain names

The dispute about the construction of the claim term "secure domain name service" (or "SDNS" for short) is whether the term admits of a broader construction than the detailed description of the preferred embodiment in the specification. VirnetX's proposed construction properly defines the term without importing unwarranted limitations into it, unlike Microsoft's.

VirnetX's Proposed Construction. The claim language is instructive. The claims say "… the query message requesting from the secure domain name service a secure computer network address corresponding to the secure domain name; receiving from the secure domain name service a response message containing the secure computer network address corresponding to the secure domain name." According to the claim language, the SDNS is capable of providing a secure computer network address in response to a query message containing a secure domain name. The specification is consistent. *'180 patent* at 6:22-36; 7:19-28; 7:29-42; 51:29-45; 51:46-52; 52:4-26; 52:27-40; 52:41-54; 53:8-17; *see also id.* at 52:55-53:7. So is the prosecution history. *Ex.* 26 at 10-11; *Ex.* 27 at 2. So the SDNS is a service that receives requests for secure computer network addresses corresponding to secure domain names, and is capable of providing the responses, as VirnetX proposes.

The specification also supports VirnetX's proposal that the SDNS responses are "trustworthy." The SDNS is capable of providing trustworthy responses, *e.g.*, by replying with the secure computer network address using a VPN link.



> Alternatively, the query to SDNS 3313 can be in the clear, and SDNS 3313 and gatekeeper 3314 can operate to establish a VPN communication link to the querying computer for sending the reply.

'180 patent at 52:51-54; *see also id.* at 51:46-50. The above shows that the SDNS can provide a trustworthy response by sending the response to the SDNS query over a VPN communication link (encrypted), which provides some assurance that there was no tampering with the response. *See id.* at 1:50-57 (describing use of encryption "in this context" to provide "security"). Moreover, in another portion highlighting the ability of the SDNS to provide trustworthy responses, the specification describes that the SDNS may verify the authority of the requestor to obtain the secure computer network address from the SDNS through various techniques. *Id.* at 51:46-50; 52:6-26; 52:41-46. The SDNS may also provide further assurances of trustworthy responses by checking that information associated with a secure domain name (*e.g.*, registered owner and secure computer network address) is provided to the SDNS. *Id.* at 53:26-54:6.

Microsoft's Proposed Construction. Microsoft's proposal repeats its erroneous limitations for "domain name" and "domain name service (DNS)" in the '135 patent, as well as its excessively limiting "secure computer network address" and "nonstandard top-level domain names." Microsoft cannot simply parse the words in this SDNS term by separately construing "secure" and "domain name service" or "domain name" from the '135 patent, and then combine these definitions to arrive at the definition of the whole term "secure domain name service" in the '180 patent. *See Warner-Lambert*, 503 F.3d at 1264. This creates an internal conflict in Microsoft's construction. Microsoft's proposal simply does not make any sense in the context of the disclosure of the '180 patent. Under Microsoft's construction, a SDNS must be an IETF standard DNS (as incorrectly construed by Microsoft for the '135 patent) but handle "non-standard" domain names. This is confusing.

Microsoft's proposal is also contrary to claim differentiation, requiring a "top-level domain name" as it does. The independent claims with the SDNS term do not recite any "top-level domain name," whereas dependent claims 11, 27 and 41 do contain that limitation.

Moreover, Microsoft's arguments that the "secure domain name service" is limited to standardized DNS as defined by the IETF are belied by the arguments the inventors made to the Patent Office during prosecution. The inventors argued that what is important is the SDNS functionality, not which entities are performing the functionality. *Ex.* 26 at 10-11 ("…what is claimed is the receiving and processing of such information, not that the method can only receive such information from certain specified entities") (emphasis added).

Microsoft argues that the patent describes the "present invention" as handling secure, "non-standard" domain names. *JCC Exh. E* ¶58 (citing 7:19-42; 51:29-52:3). These portions of the specification describe many aspects of embodiments of the "present invention," some of which are simply not claim limitations. *E.g.*, *'180 patent* at 6:8-21; 6:37-7:18. The claims do not use the word "non-standard," and the specification references cited by Microsoft do not contain lexicography or a clear disclaimer or disavowal limiting SDNS to handling "non-standard" domain names.

VirnetX's proposed construction should be adopted over Microsoft's because it is supported by the intrinsic evidence and describes the capabilities of a SDNS without unduly limiting the claim to the preferred embodiment, unlike Microsoft's.

VII. CONCLUSION

For these reasons, VirnetX respectfully requests that the Court adopt VirnetX's proposed claim constructions.

Dated: December 30, 2008

By:

/s/ Fay E. Morisseau
Otis W. Carroll (Texas Bar No. 03895700)
Deborah Johnson Race (Texas Bar No. 0016448700)
IRELAND, CARROLL & KELLEY, P.C.
6101 South Broadway, Suite 500
Tyler, Texas 75703
Telephone: (903) 561-1600
Facsimile: (903) 581-1071
Email: Fedserv@icklaw.com

Robert M. Parker (Texas Bar No. 15498000)
Robert C. Bunt (Texas Bar No. 00787165)
PARKER, BUNT & AINSWORTH, P.C.
100 East Ferguson, Suite 1114
Tyler, Texas 75702
Telephone: (903) 531-3535
Facsimile: (903) 533-9687
E-mail: rmparker@pbatyler.com
E-mail: rcbunt@pbatyler.com

Of Counsel:

Fay E. Morisseau (Texas Bar No. 14460750)
Daniel R. Foster (Pro Hac Vice)
Christopher D. Bright (Pro Hac Vice)
McDERMOTT WILL & EMERY LLP
18191 Von Karman Avenue, Suite 500
Irvine, California 92612-7108
Telephone: (949) 851-0633
Facsimile: (949) 851-9348
E-mail: fmorisseau@mwe.com
E-mail: dfoster@mwe.com
E-mail: cbright@mwe.com

David M. Beckwith (Pro Hac Vice)
McDERMOTT WILL & EMERY LLP
4370 La Jolla Village Drive
Telephone: (858) 643-1400
Facsimile: (858) 597-1585
E-mail: dbeckwith@mwe.com

Vera M. Elson (Pro Hac Vice)
McDERMOTT WILL & EMERY LLP
3150 Porter Drive
Palo Alto, CA 94304
Telephone: (650) 813-5000
Facsimile: (650) 813-5100
E-mail: velson@mwe.com

Attorneys for Plaintiff VirnetX Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on December 30, 2008.

/s/ Fay E. Morisseau
Fay E. Morisseau